

ABSTRACT OF THE DISCLOSURE

A system and method for performing source path isolation in a network. The system comprises an intrusion detection system (IDS), a source path isolation server 5 (SS1) and at least one router configured to operate as a source path isolation router (SR1) operating within an autonomous system. When IDS detects a malicious packet, a message is sent to SS1. SS1 in turn generates a query message (QM) containing at least a portion of the malicious packet. Then, QM is sent to participating routers located one hop away. SR1 uses the query message to determine if it has observed the malicious 10 packet by comparing it with locally stored information about packets having passed through SR1. SR1 sends a reply to SS1, and SS1 uses the reply to identify the ingress point into the network of the malicious packet.

15